

## **PRIVACY NOTICE FOR WHISTLEBLOWERS – DATA PROCESSING INFORMATION**

### **PRIVACY NOTICE PURSUANT TO ARTICLES 13-14 OF REGULATION (EU) 2016/679 (GDPR) IN THE CONTEXT OF THE WHISTLEBLOWING POLICY**

This privacy notice is provided by **STERCHELE SPA** (hereinafter referred to as the “Company”), in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 (General Data Protection Regulation – “GDPR”), regarding the processing of personal data collected by the Company under its **Whistleblowing Policy**, adopted in compliance with Legislative Decree No. 24 of March 10, 2023, and specifically concerning all activities and requirements related to the operation of the company’s whistleblowing management system.

This information is provided to whistleblowers as well as any other potentially “data subjects”, such as individuals mentioned as possible perpetrators of misconduct, any “facilitators” (as defined by the applicable legislation), and any other parties involved in the Whistleblowing Policy.

#### **1. Data Controller**

The data controller is STERCHELE SPA, represented by its legal representative pro tempore.

#### **2. Categories of Personal Data Processed and Purposes of Processing**

In accordance with applicable regulations, personal data may be collected by the Company as part of whistleblowing reports and any attached documentation, submitted through the reporting channels defined in the Whistleblowing Policy.

Depending on the content of the reports, the following categories of personal data may be processed:

- **a)** Common personal data (Art. 4, point 1 of the GDPR), such as name, surname, date and place of birth, contact details (phone number, postal or email address), job role/position.
- **b)** Special categories of personal data (Art. 9 of the GDPR), such as data concerning health, political opinions, religious or philosophical beliefs, sexual orientation, or trade union membership.
- **c)** Data relating to criminal convictions and offences (Art. 10 of the GDPR).

The Company recommends that whistleblowers avoid including unnecessary special category or judicial data unless strictly relevant to the report, in compliance with Article 5 of the GDPR.

The data will be processed to perform the necessary investigations regarding the reported facts and to adopt any consequent measures.

Furthermore, data may be processed for the purposes of protecting the Company's rights in judicial, administrative, or extrajudicial proceedings, including civil, administrative, or criminal disputes arising from the report.

### **3. Legal Basis of Data Processing**

The primary legal basis for processing personal data consists of the fulfilment of a legal obligation to which the Data Controller is subject – Article 6, paragraph 1, letter c) of the GDPR – which, specifically, pursuant to the above-mentioned legislation, is required to implement and manage dedicated information channels for receiving reports of unlawful conduct harmful to the integrity of the Company and/or the public interest.

In the cases provided for by the same legislation, specific and free consent may be requested from the reporting party – pursuant to Article 6, paragraph 1, letter a) of the GDPR – specifically when it is deemed necessary to disclose their identity, or in case of recording reports collected orally, by telephone or via voice messaging systems, or through direct meetings with the person responsible for managing the reports.

The processing of “special category” personal data, possibly included in reports, is based on the fulfilment of obligations and the exercise of specific rights of the Data Controller and the data subject in the field of labour law, pursuant to Article 9, paragraph 2, letter b) of the GDPR.

Regarding the purpose of establishing, exercising or defending a right in legal proceedings, the related legal basis for the processing of personal data is the legitimate interest of the Data Controller to this effect, pursuant to Article 6, paragraph 1, letter f) of the GDPR; for the same purpose, the processing of “special category” personal data, if present, is based on Article 9, paragraph 2, letter f) of the GDPR.

### **4. Nature of Data Provision**

The provision of personal data is optional, considering the possibility of submitting anonymous reports to the Company, provided they contain precise, consistent and adequately detailed information, without prejudice to what is established by the applicable regulations regarding protective measures for whistleblowers.

If provided, personal data will be processed to manage the report according to the limits and confidentiality guarantees imposed by the relevant legislation.

### **5. Methods and Retention Period of Personal Data Processing**

The processing of personal data included in reports submitted in accordance with the Whistleblowing Policy will be carried out by “authorised persons” appointed by the Company and will comply with the principles of fairness, lawfulness and transparency referred to in Article 5 of the GDPR.

Personal data processing may be carried out using analogical and/or IT/telematic methods, suitable for storing, managing and transmitting data, always applying appropriate physical, technical and organisational measures to ensure their security and confidentiality throughout every stage of the procedure, including the storage of the report and related documents – without prejudice to the provisions of Article 12 of Legislative Decree No. 24/2023 – with particular regard to the identity of the reporting party, of the persons involved and/or mentioned in the reports, of the content of the reports and related documentation.

Reports received by the Company, together with any attached documents, will be retained for the time necessary to manage them and, in any case, as provided by law, for a period not exceeding **five years** from the date of the final outcome communication. After this period, reports will be deleted from the system or stored in anonymised form.

Consistent with the indications provided in paragraph 1, personal data included in reports that are clearly irrelevant will be immediately deleted.

## **6. Data Communication and Transfer**

In addition to the aforementioned internal personnel specifically authorised by the Data Controller, personal data collected may also be processed, within the framework of the Whistleblowing Policy and for the purposes indicated, by the following third parties, formally appointed as Data Processors where the conditions of Article 28 of the GDPR are met:

- providers of consulting and assistance services for the implementation of the Whistleblowing Policy;
- IT companies and professionals concerning the application of adequate technical and organisational security measures regarding the information processed by the corporate system.

Where applicable, personal data may be transmitted to judicial authorities and/or law enforcement agencies upon request in the context of legal investigations.

Under no circumstances will personal data be subject to dissemination.

## **7. Data Subject Rights**

Each data subject has the right to exercise the rights referred to in Articles 15 et seq. of the GDPR, in order to obtain from the Data Controller, for example, access to their personal data, rectification or erasure of the same or restriction of processing, without prejudice to the right to lodge a complaint with the Supervisory Authority (Garante per la protezione dei dati personali).

To exercise these rights, a specific request must be sent in free form to the following address: **comunicazione@sterchelegroup.com**, or the form available on the website of the Italian Data Protection Authority may be transmitted to the same address.

In this regard, it should be noted that the aforementioned rights of data subjects may be restricted pursuant to and for the purposes of Article 2-undecies of Legislative Decree No. 196 of June 30, 2003 ("Privacy Code", as amended by Legislative Decree No. 101/2018), for the time and within the limits in which such restriction constitutes a necessary and proportionate measure, where their exercise could result in a concrete and actual prejudice to the confidentiality of the identity of whistleblowers.

In such cases, data subjects may still refer to the Supervisory Authority to assess whether the conditions exist to act in the manner provided for by Article 160 of Legislative Decree No. 196/2003.